🛠️ Ejercicio Práctico

📌 **Título:** *Diseño de una Solución Conectada para una Fábrica Inteligente*

🎯 Objetivo del ejercicio:

Aplicar los conceptos de tecnologías de red, automatización, comunicación M2M e Industria 4.0 mediante la simulación del diseño básico de una infraestructura conectada para una pequeña planta de producción.

📝 Instrucciones:

Imagina que eres parte del equipo de innovación tecnológica de una empresa manufacturera que desea modernizar su planta mediante tecnologías de red. Tu tarea es:

1. **Identificar tres tecnologías de red clave** que implementarías en la fábrica para lograr una automatización eficiente.

2. **Describir cómo integrarías sensores, máquinas y sistemas de control** para lograr comunicación M2M.

3. Proponer un **ejemplo concreto de uso de red 5G o IoT** en un proceso productivo (por ejemplo: ensamblaje, monitoreo de calidad, logística interna).

4. Incluir una breve reflexión sobre los posibles **riesgos de ciberseguridad** asociados y cómo los enfrentarías.

🧠 Pauta orientadora (para guiar la respuesta):

- **Tecnologías posibles a incluir:** Redes IoT, RFID, redes 5G, plataformas en la nube, M2M, sensores inteligentes.

- **Ejemplo de uso práctico:** Un sensor en cada línea de ensamblaje envía datos a un sistema central en tiempo real, que detiene automáticamente la producción si detecta una desviación de calidad.

- **Riesgos comunes:** Acceso no autorizado a la red, pérdida de datos, fallas de conectividad.

- **Soluciones posibles:** Firewalls industriales, segmentación de red, cifrado de datos.

✅ Resultado esperado:

Un esquema o texto explicativo (puede ser acompañado por un diagrama simple) que muestre la comprensión del rol de las tecnologías de red en un entorno industrial automatizado.

✅ Ejemplo de Solución: Diseño de una Solución Conectada para una Fábrica Inteligente

---

📡 1. Tecnologías de red clave a implementar:

1. **IoT Industrial (IIoT):**
   Permitiría conectar sensores y dispositivos inteligentes en toda la planta, desde la línea de producción hasta los almacenes.

2. **Redes 5G privadas:**
   Brindarían baja latencia y alta capacidad de conexión simultánea entre máquinas, ideal para entornos con múltiples procesos automatizados.

3. **Plataforma en la nube + Edge Computing:**
   Serviría para almacenar, procesar y visualizar los datos generados por la planta en tiempo real, combinando capacidad centralizada y procesamiento en el borde para respuestas rápidas.

🤖 2. Comunicación M2M en la planta:

Se instalarían sensores inteligentes en cada máquina crítica (prensas, cortadoras, brazos robóticos). Estos sensores transmitirían constantemente

datos de temperatura, vibración y rendimiento a un **controlador central (PLC)** conectado a una plataforma en la nube.

- Las máquinas estarían interconectadas por una **red interna segmentada** con soporte 5G, que permite a los equipos coordinarse sin intervención humana.

- Por ejemplo, si un sensor detecta una anomalía en el motor de una prensa, automáticamente se envía una señal al brazo robótico para detener el flujo de piezas y activar una rutina de mantenimiento.

⚙️ 3. Ejemplo práctico de uso de 5G o IoT:

Monitoreo de calidad automatizado con visión artificial e IoT:

Una cámara conectada a la red IoT revisa cada producto ensamblado y, mediante algoritmos de visión computacional, identifica posibles defectos.
Si se detecta una falla, el sistema:

- Detiene la línea en tiempo real usando comunicación M2M.

- Informa al operario a través de una plataforma web conectada vía 5G.

- Registra el evento en la nube para análisis posteriores.

Esto mejora la eficiencia y reduce pérdidas por productos defectuosos.

🔐 4. Riesgos de ciberseguridad y cómo mitigarlos:

Riesgos identificados:

- Acceso no autorizado a la red interna de la fábrica.

- Intercepción o alteración de datos entre sensores y controladores.

- Ataques a la disponibilidad del sistema (DoS).

Medidas de mitigación:

- Implementar **firewalls industriales y segmentación de red** entre zonas críticas.

- Aplicar **cifrado TLS** para todos los datos transmitidos por sensores.

- Activar **autenticación multifactor (MFA)** para acceder a la plataforma de control.
- Realizar auditorías y pruebas de penetración periódicas.
